IN THE CLAIMS

A complete list of claims is presented below with amendments marked up:

Listing of the Claims:

1-51. (Canceled).

52. (New) A computerized method of establishing a secure wireless communication channel between an access point and a station, the channel being encrypted with a channel key, the method comprising:

the access point receiving a connection request from the station to initiate a setup connection between the access point and the station;

the access point sending a shared key to the station in response to the connection request if the access point is capable of handling a connection to the station;

the access point selecting a secret access point key subsequent to sending the shared key;

the access point generating a self-distributed key using the secret access point key;

the access point generating a first value using the secret access point key and a second value from the station, wherein the second value has been generated by the station using a secret station key;

the access point sending the first value to the station, wherein the station uses the first value and the secret station key to calculate the self-distributed key;

the access point receiving an encrypted user name and an encrypted password from the station, wherein the station has encrypted the user name and the password with the self-distributed key; and

the access point decrypting the user name and the password to check for validity.

53. (New) The method of claim 52, further comprising:

the access point encrypting the channel key using the self-distributed key if the user name and the password are valid; and

the access point sending the encrypted channel key to the station to cause the station to terminate the setup connection and to establish a secured connection with the access point using the channel key.

54. (New) The method of claim 52, wherein the access point generating the self-distributed key using the secret access point key comprises:

the access point executing a security algorithm to generate the self-distributed key using the secret access point key.

55. (New) The method of claim 54, wherein the security algorithm comprises $g^n \ mod \ p$.

56. (New) A computerized method of establishing a secure wireless communication channel between an access point and a station, the channel being encrypted with a channel key, the method comprising:

the station sending a connection request to the access point to initiate a setup connection between the access point and the station;

the station sending a shared key from the access point in response to the connection request if the access point is capable of handling a connection to the station;

the station generating a first value using a secret station key;

the station sending the first value to the access point, wherein the access point uses the first value and secret access point key to generate a second value;

the station receiving the second value from the access point;

the station using the second value and a secret station key to calculate a self-distributed key previously generated by the access point using the secret access point key;

the station encrypting a user name and a password with the self-distributed key; and

sending the encrypted user name and encrypted password to the access point to be validated.

57. (New) The method of claim 56, further comprising:

the station receiving the channel key in an encrypted form from the access point if the user name and the password are validated by the access point; and

the station decrypting the encrypted channel key using the self-distributed key.

58. (New) The method of claim 57, further comprising:

the station terminating the setup connection; and

the station establishing a secured connection with the access point using the channel key decrypted.

59. (New) The method of claim 56, wherein the access point executes a security algorithm to generate the self-distributed key using the secret access point key.

60. (New) The method of claim 59, wherein the security algorithm comprises $g^n \bmod p$.

61. (New) A computer-readable medium having stored thereon executable instructions to cause a processor to perform a method for establishing a secure wireless communication channel between an access point and a station, the channel being encrypted with a channel key, the method comprising:

the access point receiving a connection request from the station to initiate a setup connection between the access point and the station;

the access point sending a shared key to the station in response to the connection request if the access point is capable of handling a connection to the station;

the access point selecting a secret access point key subsequent to sending the shared key;

the access point generating a self-distributed key using the secret access point key;

the access point generating a first value using the secret access point key and a second value from the station, wherein the second value has been generated by the station using a secret station key;

the access point sending the first value to the station, wherein the station uses the first value and the secret station key to calculate the self-distributed key;

the access point receiving an encrypted user name and an encrypted password from the station, wherein the station has encrypted the user name and the password with the self-distributed key; and

the access point decrypting the user name and the password to check for validity.

62. (New) The computer-readable medium of claim 61, the method further comprising:

the access point encrypting the channel key using the self-distributed key if the user name and the password are valid; and

the access point sending the encrypted channel key to the station to cause the station to terminate the setup connection and to establish a secured connection with the access point using the channel key.

63. (New) The computer-readable medium of claim 61, wherein the access point generating the self-distributed key using the secret access point key comprises:

the access point executing a security algorithm to generate the self-distributed key using the secret access point key.

64. (New) The computer-readable medium of claim 63, wherein the security algorithm comprises $g^n \ mod \ p$.

65. (New) A computer-readable medium having stored thereon executable instructions to cause a processor to perform a method for establishing a secure wireless communication channel between an access point and a station, the channel being encrypted with a channel key, the method comprising:

the station sending a connection request to the access point to initiate a setup connection between the access point and the station;

the station sending a shared key from the access point in response to the connection request if the access point is capable of handling a connection to the station;

the station generating a first value using a secret station key;

the station sending the first value to the access point, wherein the access point uses the first value and secret access point key to generate a second value;

the station receiving the second value from the access point;

the station using the second value and a secret station key to calculate a self-distributed key previously generated by the access point using the secret access point key;

the station encrypting a user name and a password with the self-distributed key; and

sending the encrypted user name and the encrypted password to the access point to be validated.

66. (New) The computer-readable medium of claim 65, the method further comprising:

the station receiving the channel key in an encrypted form from the access point if the user name and the password are validated by the access point; and

the station decrypting the encrypted channel key using the self-distributed key.

67. (New) The computer-readable medium of claim 66, the method further comprising:

the station terminating the setup connection; and

the station establishing a secured connection with the access point using the channel key decrypted.

68. (New) The computer-readable medium of claim 65, wherein the access point executes a security algorithm to generate the self-distributed key using the secret access point key.

69. (New) The computer-readable medium of claim 68, wherein the security algorithm comprises $g^n \bmod p$.

70. (New) A secure wireless network comprising:

a station operable for sending a connection request to initiate a setup connection and for generating a first value using a secret station key;

an access point wirelessly and communicably coupled to the station, the access point operable for sending a shared key to the station in response to the connection request if the access point is capable of handling a connection with the station, for selecting a secret access point key subsequent to sending the shared key, for generating a self-distributed key using the secret access point key, for generating a second value using the secret access point key and the first value from the station, and for sending the first value to the station, wherein the station is further operable for calculating the self-distributed key using the second value and the secret station key, for encrypting a user name and a password with the self-distributed key, and for sending the encrypted user name and the encrypted password to the access point to be validated.

71. (New) The network of claim 61, wherein the access point is further operable for encrypting a channel key using the self-distributed key if the user name and the password are validated and for sending the encrypted channel key to the station.

72. (New) The network of claim 62, wherein the station is further operable for decrypting the encrypted channel key using the self-distributed key, for terminating the setup connection, and for establishing a secured connection with the access point using the channel key.